February 20, 2020

To Whom It May Concern:

Digital Aerolus, Inc. ("Digital Aerolus" or "DA") a Kansas aerospace engineering company, designs flight control systems for vehicles. We produce commercial inspection UAVs that navigate stably indoors and underground without GPS and other external sensors.

The Federal Aviation Administration's ("FAA") Remote ID NPRM affects both drone users and manufacturers. The language of the NPRM limits US drone users to hardware that conforms to the Remote ID rule and constrains US manufacturers from designing UAVs that do not continuously signal their presence to the internet.

We design UAVs that fly where there is no GPS or internet, and where conventional UAVs can't navigate: in airspaces not traditionally subject to FAA regulation, and where location services and internet signals required for Remote ID are not accessible. Conventional drones, including the market-predominant models from China, are optimized to fly outdoors, and routinely depend on location services and the internet. Digital Aerolus drones fly stably in spaces that defeat the navigation systems of these conventional drones.

Digital Aerolus has demonstrated that the market is substantial for US-made indoor and underground UAVs. Multiple market sectors use our products, including bridge inspectors, mine operators, police and emergency teams, and the energy industry including nuclear. Our Aertos UAVs perform DOT inspections of highway infrastructure, complete border tunnel surveys for DHS, and explore wilderness caverns for the Travel Channel.

We're committed to continuing to develop technology solutions that improve security, increase safety, protect lives, promote commerce, and create jobs. We design and build our products in the US, and our technology is protected by numerous granted and in-process US patents. We built our Folded Geometry Flight Code™ (FGC™) and Mind of Motion autonomous Framework™ (MMF™) from the ground up. We believe these technologies will serve as the foundational software framework for the next generation of UAVs and autonomous vehicles.

But the Remote ID rule, as written, significantly impedes our business, effectively shuts down the indoor inspection UAV industry, and places limits on innovation by companies in the USA. While the goals of remote ID are well intentioned, this proposed implementation clouds the very definition of where the FAA's authority starts and stops with regards to airspace. As written, this rule would effectively give the FAA jurisdiction of the airspace inside buildings, factories, pipes, mines, culverts, tunnels, and underground wiring infrastructure, as well as near building and highway infrastructure, for various first responder applications, and in many other confined spaces.

Digital Aerolus implores you to help us by:

- Reading this Position Statement to understand our position;
- Reviewing our proposed revisions to the Remote ID Rule's language;
- Modifying the NPRM language, and/or create categorical exceptions for industry innovators like Digital Aerolus;
- Clarifying what is FAA-regulated airspace; and
- Standing with us to protect US innovation and to promote national security, safety, and a reasonable Remote ID rule.

Respectfully,

Digital Aerolus, Inc.
Lenexa, Kansas, USA

POSITION STATEMENT
COMMENTS ON FAA'S PROPOSED REMOTE ID RULE
NPRM 84 FR 72438 FAA-2019-1100

DIGITAL AEROLUS, INC.
LENEXA, KANSAS, USA

SUBMITTED TO THE FAA
BY DIGITAL AEROLUS, INC.

TABLE OF CONTENTS

INTRODUCTION:

Digital Aerolus, Inc. ("Digital Aerolus" or "DA") an aerospace technology company, objects to the foundation and substance of the proposed Remote ID "Remote ID Rule" set forth in the Notice of Proposed Rulemaking ("NPRM") issued by the FAA on December 31, 2019.

The FAA's stated intent in proposing the Remote ID Rule is to ensure public safety and security, and the safety and efficiency of the airspace of the United States ("US"). We embrace the spirit and intent of the Remote ID Rule. As aerospace professionals and pilots, we understand why the FAA believes that UAVs flying in FAA-regulated airspace should have identifiers and we support Remote ID as a step forward towards integrating UAVs into FAA-regulated airspace and help ameliorate the conflicting demands of manned aircraft, UAV operators, Federal security partners, and the general public.

But the FAA exceeds its rulemaking authority in the NPRM to the extent it imposes restrictions on UAVs not operating in FAA-regulated airspace and on manufacturing designs for such types of UAVs, such as inspection drones flying indoors, in tunnels, in mines, and in other industrial environments that are generally not within FAA-regulated airspace. These are all locations that often do not have access to GPS or internet signals yet are use cases that have seen dramatic improvements in that increase public safety and security through the use of UAVs to increase the frequency, thoroughness, and visual records of reviews and inspections of this critical industrial infrastructure.

The proposed Remote ID Rule, as set forth in the NPRM, unnecessarily invites litigation challenging the FAA's rulemaking authority, which could impose a burden on the FAA and delay implementation of the Remote ID Rule as to UAVs flying in FAA-regulated airspace. The Remote ID Rule as presently proposed in the NPRM bans the manufacture of UAVs designed for industry use outside FAA-regulated airspace and would substantially reduce their use in these areas that have seen extensive economic and public safety benefits to date. This, in turn, will cripple the growing industrial UAV industry in the US, and will inhibit the safety, security, and efficiency that UAVs provided for these and other commercial sectors. This works against the intent of the NPRM and impedes development critical to US industries.

(NPRM: FAA–2019–1100; Remote Identification of Unmanned Aircraft Systems)

OVERVIEW:

Digital Aerolus, an aerospace technology firm in Lenexa, Kansas, engineers and manufactures a patented flight control system for UAVs and other vehicles that require control systems which are able to operate fully independent of traditional navigational aids such as GPS, VOP, LORAN, magnetic bearings, optical flow, or similar systems. DA's control systems for pilot-operated and autonomous vehicles increase utility, efficiency, safety, and security, and will continue to advance the next generation of autonomous and intelligent drones, automobiles, submarines, submersibles, and ground robots.

The company's first products are the Aertos inspection drones. Unlike conventional UAVs, Aertos drones achieve stable, predictable flight without referring to GPS satellite signals or the internet. Thus, Aertos drones created a new industry: UAVs that can conduct flights into environments that don't have access to traditional navigational aids, including GPS or the internet, and in environments that are generally outside of FAA-regulated airspace.

By way of example, Aertos drones recently completed successful missions where conventional drones cannot fly: indoors, inside energy plants and warehouses, underground in caves, through tunnels, and in mines. And, unlike conventional drones, Aertos drones successfully fly in proximity to steel, metal, concrete, rock, and other materials that have historically prevented UAVs from operating. And, if the FAA modifies the Remote ID Rule as described in Section V so as to not apply to UAVs operating outside FAA-regulated airspace, DA anticipates the market for such confined space platforms will exceed $500M in sold devices over the next 5 years.

As written, the proposed Remote ID Rule requires manufacturers to engineer, into every UAS, Remote ID, USS communication capabilities, and GPS location abilities. The Remote ID Rule mandates a UAS design that prevents launch when Remote ID does not function completely. These Remote ID Rules apply to all UAS devices, not just those designed to fly in FAA-regulated airspace. We provide UAVs to industries that need UAS for uses outside FAA-regulated airspace and depend on rapid launch and stable navigation without referring to GPS location signals or the internet. Thus, the Remote ID Rule as proposed in the NPRM would severely and immediately harm opportunities to advance efficiency, safety, and security in autonomous and remote vehicles across multiple industries. In Section 5, we propose modest edits that would allow the continued manufacture, development and use of UAS for industry purposes that involve flight in GPS- and internet-compromises areas not in FAA-regulated airspace while preserving the Remote ID rule as applied to FAA-regulated airspace.

By basing Remote ID on how conventional drones operate, by presuming that future UAVs must connect to location services such as GPS merely because the present generation of technology principally relies on such technology, and by limiting manufacturers to UAV designs that have this capability, the FAA would stifle innovation by US companies, compromise its stated objective of increasing safety and security with Remote ID, and confuse airspace regulated by the FAA with unregulated spaces indoors and underground.

ISSUES & DISCUSSION:

Issue 1: The Remote ID Rule bans manufacture and use of UAVs that operate in non-FAA-regulated airspaces that have compromised GPS, USS communication, and internet connectivity, and thereby eliminate the availability of this technology for a broad range of industry uses that increase safety and security for workers and for the public.

Discussion: DA builds UAS that specifically are intended to operate in GPS-compromised environments outside FAA-regulated airspace, including:

- Inside reinforced concrete structures that have steel reinforcing bars;
- Beneath metal roofing;
- In close proximity to concrete walls and ceilings;
- Underneath bridge decks;
- In and through culverts and tunnels;
- Inside storm sewer and wastewater lines;
- In underground storage facilities and warehouses;
- In chimneys, mine shafts, and caverns; and
- In other areas where the heading of the UAV based on magnetic bearings is not unavailable.

The Remote ID Rule requires DA to design remote identification into every drone, and requires DA drones to communicate location by GPS or the internet to an approved USS (UAS service supplier).

Specifically, the rule requires all drones to:

- Automatically connect to a USS, and
- Continually indicate latitude, longitude, and barometric pressure altitude of the control station and/or aircraft.

Unlike conventional aircraft, DA UAVs do not rely on GPS, optical flow, or magnetic fields for stable flight. GPS signals, with wavelengths of ~190 mm and ~244 mm, generally require an uninterrupted line of sight from the UAV to the sky, and do not penetrate metal or soil.

DA specifically designs UAVs to navigate in environments where GPS signals and internet services may not be available. These environments will similarly compromise internet-based USS communication.

Under both standard and remote identification categories, all DA drones must self-test and monitor for USS connectivity before each launch and during each flight. Since DA aircraft operate in environments where GPS signals are absent or unavailable, and fly outside the specific geographic areas where certain exceptions are allowed, DA UAVs would be unable to launch under the Remote ID performance requirements.

Specifically, subpart F of the Remote ID Rule specifies the requirements for the design and production of UAS operated in the United States. Under these proposed rules:

- DA unmanned aircraft do not fall under any of the exceptions listed in § 89.501(c);
- In typical and intended operation for and by our customers, DA aircraft cannot meet the requirements listed in § 89.510(a)(1);
- DA UAVs cannot be labeled as required in § 89.515; and
- DA UAVs will not qualify for the submission of a declaration of compliance under § 89.520

Issue 2: The Remote ID Rule places restrictions on US manufacturers of UASs that do not operate in FAA-regulated airspace. Unregulated airspace is beyond the scope of the FAA's rulemaking authority.

Discussion: UAVs from DA operate in environments that are rarely inside airspaces regulated by the FAA. This includes indoors, underground, and inside energy facilities, mines, tunnels, tanks, and chimneys. As written, the FAA rule places restrictions on manufacturers of a UAS system that will never enter FAA-regulated airspace.

As a US manufacturer of UAVs, DA is compelled to comply with FAA airspace requirements in the UAVs that DA manufactures, including those designed to primarily operate outside FAA-regulated airspace, but which may operate inside FAA-regulated airspace during some missions or parts of missions.

We contend that these restrictions are beyond the manufacturer's responsibility or capability, and requiring them is beyond the FAA's authority.

Issue 3: DA's strategy for developing flight control systems will advance safety and security, the two primary objectives of the FAA Remote ID rule. The rule as written places obstacles for both security and safety.

Discussion: DA engineers its technology in Kansas, USA, a state that exceeded $3B in aerospace exports last year. DA designs aircraft that fly stably and predictably within non-regulated airspaces. Using drones instead of humans for dangerous tasks in risky environments increases efficiency and keeps workers safe.

DA's business objectives specifically align with Title 1 of the USA PATRIOT Act (2001). Title 1 authorizes measures that enhance domestic security against terrorism.

The 2020 UAV market is dominated by foreign manufacturers, particularly from China. These manufacturers build hardware that (a) predominantly require GPS, and (b) communicate information across servers controlled by the manufacturer. The US Federal Government is concerned that the current generation of Chinese internet-connected drones potentially compromise national security.

On January 29, 2020, the US Department of Interior (DOI) disallowed all operations of Chinese drones in its fleet due to cybersecurity concerns and its stated mission to protect sensitive information about US infrastructure. This action essentially grounded the entire DOI drone fleet.

DA's mission is to design and manufacture drones and other vehicles in the United States that use secure, segregated control systems independent of communication links or cloud servers located in or controlled by foreign countries. The Remote ID rule as written compromises DA's efforts to advance security and safety in the USA and impedes an entire indoor inspection industry aligned with the stated goals of the FAA, the DOI, and USA PATRIOT Act HR 3162.

Issue 4: Requiring every drone to connect to USS and location services before launch compromises safety, and may be a significant cybersecurity vulnerability.

Discussion: A foreign entity intent on harming the USA might attempt to deny service across the USS by using a DOS flood attack, by compromising DNS, or through another means. This represents a single point of failure risk.

If multiple USS were simultaneously compromised, all drones would immediately be grounded because they cannot connect to the internet. This would include, for example, every US UAV on an industrial safety or an emergency response mission. Adding a no-exception USS requirement for every manufactured drone thus represents a security vulnerability. In addition, forcing humans to perform tasks that drones could easily complete, especially during life-at-risk critical emergencies when minutes or hours are wasted because UAVs cannot launch, is a huge safety opportunity cost.

NOTIONAL SCENARIOS:

The NPRM includes notional scenarios as examples of how the FAA envisions the Remote ID Rule would apply to certain common situations.

DA proposes these additional notional scenarios. They serve as additional examples to illustrate how the Remote ID Rule proposed on the NPRM might apply to certain situations common to UAVs designed to operate in non-FAA-regulated airspaces.

Notional Scenario 1: UAV Inspects a Highway Tunnel

Adam is a licensed drone pilot. His commercial inspection drone, unlike drones designed to fly in FAA-regulated airspace, navigates without connecting to GPS or the internet.

In conjunction with the State Department of Transportation, he carries the drone into the ventilation system of a major US highway beneath a harbor in an eastern US state. He launches the drone, and uses its camera to inspect roadways, shafts, fans, and other critical infrastructure.

Adam knows he is not flying in FAA-regulated airspace. Adam also knows that internet and GPS signals are not available inside the tunnel and the ventilation system.

Adam also knows that, under the proposed FAA Remote ID rule, his drone can only take off when he is outside the tunnel where GPS and internet signals are accessible. If he pilots the vehicle into the tunnel where his craft loses access to the internet and GPS, the rule prevents him from landing the drone for routine tasks like battery replacement, and then relaunching it.

Under the proposed FAA Remote ID rule, it's impossible for Adam to complete his mission.

(Note: this scenario describes real flights recently accomplished by an Aertos drone.)

Notional Scenario 2: Drone in a Mineral Mine

Betty directs operations for a major mineral mine in a Western state. She wants to use a drone to survey chat piles and evaluate their stability, and to inspect ventilation shafts, tunnels, and access corridors a mile underground. Using a drone for these missions supports the mine's business, resource management, and safety objectives.

Betty knows that accomplishing this task with human teams is dangerous and time-consuming. She also knows that broadcasting RF or other signals is dangerous where explosives might be in use, and that the industry rule is "no 2-way radios" near active or recent blast areas.

She arranges for a pilot to use a drone capable of navigating GPS-denied and signal-denied spaces to inspect and map the mine with high resolution cameras.

The pilot knows that the internet is not available a mile underground. He also knows that the proposed FAA Remote ID rule prevents him from launching a drone that does not connect to a USS, and disallows the manufacturer from including an option to override the restriction.

Under the proposed FAA Remote ID regulation, it's impossible for Betty and her pilot to complete her mission.

(Note: this scenario describes real flights recently accomplished by an Aertos drone.)

Notional Scenario 3: UAS Flies Underground in a Wilderness Area

Calvin produces content for a cable TV channel. His video documentary project profiles wildlife and geology in the Northeast mountain wilderness, an area without internet or cell phone access.

Calvin wants to send a camera and microphone into small caverns to listen for sounds and search for biological samples. The missions are too dangerous for a human team: the interiors are unexplored; there may be dangerous animals or poisonous gases inside; and entrances or passageways are physically too small for a human to enter.

For his documentary, Calvin contracts for a pilot to fly a drone to carry a camera and microphone into the underground caves. The pilot knows she is not flying in FAA-regulated airspace for a large fraction of the mission. She also knows that the internet is not available in the wilderness.

The pilot also knows that, under the proposed FAA Remote ID rule, she can't navigate the drone into the mouth of the cavern and then turn the drone off to allow the microphone to record sounds while the camera surveys the cave walls. If she lands the drone in the cave, the proposed FAA rule prevents her from relaunching because internet signals are not available, and she can't manually retrieve the UAV because the cave's narrow entrance and vertical descent are too dangerous for a human.

Under the proposed FAA Remote ID rule, the pilot either loses her expensive drone and camera, or risks injury or death to recover it. Calvin and his production team cannot complete their mission.

(Note: this scenario describes a series of real flights recently accomplished by an Aertos drone under the direction of the Travel Channel. USA broadcast date: 1/26/2020)

Notional Scenario 4: UAV Inspects an Energy Plant

David oversees operations for a USA energy corporation. He wants to use a drone to inspect the infrastructure and interiors inside coal, natural gas, and nuclear power plants. He knows that the overhead of deploying and managing human teams to do this under OSHA regulatory requirements is formidable, that the spaces are dangerous for humans due to impediments like dust, asbestos, and radiation, and that using a UAV for his task will protect lives.

He conducts test flights using drones from China, but observes that these UAVs require GPS for stable flight, and they are not controllable in his indoor environment dense with competing signals. David also does not want to provide information about his plant's infrastructure to cloud servers in foreign countries, particularly to those the Government has expressed concern about.

David arranges for a pilot to fly an Aertos inspection drone designed by Digital Aerolus. The pilot launches the drone and inspects coal chutes, ash boilers, corridors and other areas of the plant interior.

The flight is not conducted in FAA-regulated airspace. Under the proposed Remote ID Rule, the Aertos drone is required to be manufactured so that it cannot launch and complete the critical maintenance and safety tasks inside this energy facility because location signals and the internet are not available, and it's impossible for David to complete his mission.

(Note: this scenario describes real flights recently accomplished by an Aertos drone.)

Notional Scenario 5: Drone Flies Close to a Highway Bridge

Eric's firm contracts with the State Department of Transportation to inspect and maintain bridges and culverts supporting an interstate highway. He wants to use a camera on a drone to inspect bolts for excessive rust, and concrete for spalling, so he can recommend maintenance procedures.

Eric is a licensed drone pilot. He knows that conventional drone technology does not work for this application: some portions of the mission will lack GPS availability, and steel/rebar construction may cause magnetic fields that interfere with flight. As a conventional UAV approaches the infrastructure of a highway bridge, it is likely to fail and crash due to interference with its conventional navigational system.

Eric knows that, under the proposed FAA Remote ID rule, he cannot recover or relaunch his drone if his vehicle loses access to the internet in the signal-compromised area under the bridge, and under the proposed rule he likely cannot complete his mission. He also knows that on January 29, 2020, the US Department of Interior disallowed all operations of Chinese drones in its fleet due to cybersecurity concerns and its stated mission to maintain sensitive information about US infrastructure.

He also knows that a Standard Remote ID drone is likely to lose access to location services while flying under a bridge and would likely be stranded when relaunch is disallowed.

Eric deploys an Aertos drone from Digital Aerolus, navigates it into the GPS- and signal-denied spaces under the bridges, and completes his mission. Under the proposed FAA Remote ID rule, his drone is required to be manufactured to not launch in the absence of location services and internet signals, and therefore Eric would be unable to complete his critical maintenance tasks, and he cannot complete his mission.

(Note: this scenario is based on real flights recently accomplished by an Aertos drone.)

Notional Scenario 6: UAV Explores a Border Tunnel

Frank is an FAA-licensed pilot with experience operating a drone optimized to fly in areas where signals from GPS satellites and the internet are not available.

He receives a call from a representative of the US Department of Homeland Security. The representative explains that Immigration and Customs Enforcement will be deploying new technologies, including drones, to maintain border security. Deploying drones or other autonomous vehicles into unauthorized underground tunnels and other areas can provide information to US enforcement teams that is critical to preserving national security and/or saving lives.

DHS and ICE invite Frank to travel to a southwestern state to fly his UAV through a border tunnel and deliver visual images of its interior.

Frank knows that his drone will be exploring an unpredictable environment that is dangerous for human teams. He'll be piloting his drone BVLOS (Beyond Visual Line Of Sight) in a corridor with narrow walls where collisions are likely. He also knows that flying in this border tunnel will help him understand how the UAV responds in challenging underground environments, and supply the engineers of the US manufacturer he represents with feedback that helps them continue to design flight systems for the next generation of secure autonomous vehicles. He also understands the importance of using a secure, segregated communication method that does not pass information to any unauthorized entity, especially through an internet app or a cloud data server.

He also knows that, under the proposed Remote ID Rule, his drone is required to be manufactured to not launch in the absence of location services and internet signals that are not available in underground tunnels. The manufacturer he represents would be disallowed from designing or marketing a UAV with the capabilities he needs to complete his mission.

Eric deploys his Aertos drone, navigates it through the border tunnel, and completes his mission.

(Note: this scenario is based on real flights recently accomplished by an Aertos drone.)

Notional Scenario 7: US Aerospace Engineering Team

A US aerospace engineering Team believes that the next generation of autonomous vehicles should have intrinsically stable flight control systems that do not refer to satellite and internet signals, and that this core capability will become the baseline requirement for all autonomous vehicles.

The Team invents an advanced navigation system for vehicles. The navigation system has these features:

- Constructed upon advanced mathematical axioms deployed in USA spacecraft
- Does not connect to the internet or depend on signals from GPS satellites
- Enables stable, predictable vehicle navigation without referring to external sensors
- Allows vehicles to navigate indoors and underground, and
- Establishes a framework to develop truly autonomous navigation systems for multiple industries.

The Team patents and trademarks their Folded Geometry Flight Code™ (FGC™) navigation system and Mind of Motion autonomous Framework™ (MMF™).

To demonstrate the new system, the Team creates a line of commercial drones that carry a high-resolution inspection camera. They develop their technology in Kansas, USA, home to aerospace industry leaders including Boeing, Collins Aerospace, NIAR, NCAT, and others, that export $3B per annum.

The Team develops UAVs with the following capabilities:

- Drones that can fly stably and predictably underground, near steel and metal, over water, and in the dark
- Drones that are optimized for mission flights into airspaces not currently regulated by the FAA, and
- Drones that are not manufactured offshore, and do not rely on companies or data servers based in foreign countries

The Team's UAVs complete multiple flights in non-FAA-regulated airspaces, and the drones attract broad attention from customers across multiple industries. Team then decides to further expand sales of UAVs and develop the next generation of navigation systems that power autonomous vehicles like cars, boats, submersibles, and ground robots indoors and underground. They believe their technology will broadly advance safety, security, efficiency, and privacy, and will become the cornerstone technology for vehicle navigation.

Under the proposed FAA Remote ID rule, it's impossible for the Team to complete its mission.

(Note: this scenario is DA's reality.)

RECOMMENDED ACTIONS AND SUGGESTED REVISIONS

Digital Aerolus believes that the FAA Remote ID NPRM, as written, unfairly and unnecessarily constrains manufacturers and customers of UAVs that are designed to fly indoors and in other signal-denied areas. While this may be unintentional, the NPRM effectively extends FAA-regulated airspace to include indoor and underground environments.

We believe the FAA must revise the NPRM. The revisions below represent the minimal changes that will accommodate the existing industrial inspection UAV industry and other legitimate industries, and allow for future innovation and invention. These are the minimum removals, changes, or additions which would allow DA and other entities to continue to develop advanced technologies for industry, and to continue to operate without undue burdens on manufacturing or unfair restrictions on its customers.

DA therefore respectfully suggests the following revisions to the NPRM:

1. **Section 48.5 (a):** *Registration Under Part 47*
   Recommended Action: Modify to explicitly state that areas such as those underground or indoors are not covered by this regulation.
   Suggested Revision: "Except as provided in paragraph (b) or (c) of this section, compliance with the requirements of this part or part 47 of this chapter is required prior to operation of the small unmanned aircraft within the airspace of the United States."

2. **Section 89.101:** *Applicability of operating requirements*
   Recommended Action: Modify to explicitly state that areas such as underground or indoors are not covered by this regulation.
   Suggested Revision: "This subpart applies to the following: (a) Persons operating unmanned aircraft within the airspace of the United States registered or required to be registered under part 47 or part 48 of this chapter. (b) Persons operating foreign civil unmanned aircraft within the airspace of the United States."

3. **Section 89.110** – *Standard remote identification UAS; the introductory clause:*
   Recommended Action: Modify to explicitly state that operators flying aircraft in areas such as underground or indoors are not covered by this regulation.
   Suggested Revision: "A person operating a standard remote identification unmanned aircraft system within the airspace of the United States is responsible for complying with this section."

4. **Section 89.110** – *Standard remote identification UAS;* the end portion:
   Recommended Action: Modify to clarify that a portion of the flight outside of the airspace of the United States does not have to meet the requirements. Furthermore, "functional" should be more specifically defined regarding when remote identification equipment is deemed not functional.
   Suggested Revision: "(c) Operation of standard…. Unless otherwise authorized by the Administrator, a person may operate a standard remote identification unmanned aircraft system within the airspace of the United States only if it…." and "(2) Its remote identification

equipment is functional and complies with the requirements of this part from takeoff to landing while operating within the airspace of the United States."

5. **Section 89.115**: *Limited remote identification UAS*
   Recommended Action: Modify to clarify that the portion of the flight outside of the airspace does not have to meet the requirements.
   Suggested Revision: "A person operating a limited remote identification unmanned aircraft system within the airspace of the United States is responsible for complying with this section:"; "(a)Remote identification. Unless otherwise authorized by the Administrator, a person may operate a limited remote identification unmanned aircraft system only if, from takeoff to landing, while operating within the airspace of the United States:" and "(2) Its remote identification equipment is functional and complies with the requirements of this part from takeoff to landing as long as flown within the airspace of the United States."

6. **Section 89.305:** *Message elements broadcast and transmitted by standard remote identification UAS*
   Recommended Action: Modify to acknowledge that in circumstances when flying under bridges, underground, indoors, or other similar situations that a lack of GPS or other location service shall not prohibit the takeoff of the unmanned aircraft.
   Suggested Revision: "A standard remote identification unmanned aircraft system must transmit the following remote identification message elements through an internet connection to a Remote ID USS when available and must broadcast the following remote identification message elements…" and "(b) An indication of the latitude and longitude of the control station when available." In addition: "(d) An indication of the latitude and longitude of the unmanned aircraft when available."

7. **Also Section 89.305:**
   Recommended Action: Modify to reflect that regarding the UTC element can be imprecise. UTC in existing UAVs is typically derived from the location service to provide a synchronized time stamp. There will be discrepancies with any internally recorded system that does not synchronize when location services are unavailable.
   Suggested Revision: "(f) A time mark identifying the Coordinated Universal Time (UTC) time of applicability of a position source output as long as the location service is available."

8. **Section 89.310:** *Minimum performance requirements for standard remote identification UAS*
   Recommended Action: As above, modify to allow that a lack of GPS or other location service shall not prohibit the takeoff of the unmanned aircraft. Once again, the rule must not require location information when it is simply not available because the UAV is flying in spaces where location services are not available.
   Suggested Revision: "(a) Control station location. The location of the control station of the unmanned aircraft system must be generated and encoded into the message elements as long as the location service is available and must correspond to the location of the person manipulating the flight controls of the unmanned aircraft system."

9. **Also Section 89.310:**
   Recommended Action: This section explicitly specifies "within the airspace of the US", and also states that if the USS is not available that the UAS may still fly. When flying within certain confined spaces the internet may be available through Wi-Fi connections, but firewalls might not allow connections to a USS. Since those confined spaces may not even be within the airspace of the United States, it is an overreach of the FAA to force manufacturers to design and produce only unmanned aircraft that cannot fly in such circumstances.
   Suggested Revision: "(b) Automatic Remote ID USS connection. From takeoff to landing while in the airspace of the United States, the unmanned aircraft system must automatically maintain a connection to the internet and transmit the message elements through that internet connection to a Remote ID USS when the internet and the Remote ID USS are available."

10. **Also Section 89.310:**
    Recommended Action: Modify to clarify that UTC will only be precise and synchronized. when the location services are available
    Suggested Revision: "(c) Time mark. The time mark message element must be synchronized with all other remote identification message elements when location services are available."

11. **Also Section 89.310:**
    Recommended Action: This provision should be clarified that functional means the system is operating, not requiring that location services and time marks be available.
    Suggested Revision: "(2) The unmanned aircraft must not be able to take off when location services are available and the remote identification equipment is operating…."

12. **Also Section 89.310:**
    Recommended Action: This provision should be clarified that adding manual overrides or other functionality allowing the UAV to operate in signal denied areas in accordance with the above revisions does not constitute tampering.

13. **Also Section 89.310:** the (f) Connectivity portion
    Recommended Action: The Connectivity portion should be struck. We believe this portion of Section 89.310 is an overreach and inappropriately requires manufacturers to verify availability of the internet in each use case. Operators are licensed pilots, and they must be responsible for operating their aircraft in a safe and compliant manner. Forcing a manufacturer to disallow takeoff of the UAV due to connectivity problems with Remote ID will not increase safety: it actually presents a problem for users like industrial inspectors and public safety teams who might deploy a camera UAS from a remote location to keep workers safe, or to provide help to a person. and where internet might be available, but generally is restricted or limited for security and safety reasons. This is especially critical in emergency or disaster response situations when every second matters and internet connectivity may show as available but not functional due to overwhelming demand. In addition, immediate response is most crucial in these instances, and using a drone that turns on instantly without waiting to establish USS or internet connectivity becomes invaluable to saving a life. If the unmanned aircraft becomes unusable in certain circumstances, users will be unable to rely on them for mission critical

activities and either be unable to complete their missions or be compelled to use far more dangerous means to complete them. In many cases, the unmanned aircraft used by public safety teams will not qualify as exempt, either because the public safety teams are not employees of the United States government, or because the unmanned aircraft the teams use are not explicitly designed solely for government use.

14. **Also Section 89.310:** *"(1) The message elements in 89.305 transmitted through an internet connection to a Remote ID USS from the unmanned aircraft system and broadcast from the unmanned aircraft must be identical"*
    Recommended Action: The message elements portion should be struck. In some circumstances, the messages may not be perfectly identical, but can be easily analyzed as the same message. For example, if the location is off by a meter in a broadcast message vs. the USS connection, the intended location information is still clear, but may not exactly match. Non-identical messages could happen simply due to timing issues or to a temporary internet availability issue.

15. **Similar changes to Section 89.315:** *The "(l) Range limitation" elements*
    Recommended Action: The Range Limitation elements should be struck. In many circumstances, it makes sense to design a UAV unmanned primarily for indoor use but also for occasional outdoor flight. The unmanned aircraft should never be prohibited from operating more than 400 feet from the operator when indoors and not in FAA-regulated airspace. This is an overreach. In addition, a "(m) Broadcast limitation" is not logical. If an aircraft is limited in range yet might be broadcasting, why would it be prohibited? It is rare that enough limited range aircraft would fly in the same area to cause congestion or interference.

16. **Section 89.510:** *Design and production requirements*
    Recommended Action: Reconsider Section (a). Section (a) is an overreach when considered in the context of other sections of the proposed rule. US manufacturers currently produce Unmanned Aircraft Systems in the United States which users will not fly within the airspace of the United States. Example circumstances include UAVs that fly indoors, underground, or underneath or near bridges or other structures. The FAA should not force Remote ID rules on UAVs that are designed to fly indoors. Operators of unmanned aircraft should be responsible for their actions but forcing the design of an aircraft to prohibit flight just because Remote ID can't succeed represents a safety problem. Requiring Remote ID messaging will, for example, prevent an emergency team from using a rapid-deploy UAV that can fly inside a structure to survey for critical information that saves a life. This also restricts commercial development and constrains industries that fly missions indoors, underground and in non-regulate airspace. Adding the revisions described earlier will allow pilots to fly UAVs in circumstances where location services are unavailable. Those revisions would thus make 89.510(a) acceptable.

DIGITAL AEROLUS, INC.
9910 WIDMER ROAD
LENEXA, KANSAS USA 66215

800.894.3616
913.298.1226

www.DigitalAerolus.com

Jeffery J. Alholm, Chief Executive Officer
jeff.alholm@digitalaerolus.com

Thomas Williams, Ph.D., Chief Engineering Officer
tom.williams@digitalaerolus.com

John Blessing, Technology Architect
john.blessing@digitalaerolus.com

REFERENCES:

- FAA Remote ID NPRM – 12/31/19 (319 pages)
    - https://www.regulations.gov/document?D=FAA-2019-1100-0001

- FAA Overview of Remote ID Unmanned – 1/16/120 (14 pages)
    - https://www.regulations.gov/document?D=FAA-2019-1100-5896
    - slide show presentation to House and Senate Aviation Committee bipartisan staffs

- FAA Remote ID Regulatory Impact Analysis – 12/20/19 (190 pages)
    - "Preliminary Regulatory Impact Analysis for the Remote Identification of Unmanned Aircraft Systems NPRM"
    - https://www.regulations.gov/document?D=FAA-2019-1100-0012

- DOI Memorandum: Drones grounded upon security concerns - 1/20
    - https://www.doi.gov/pressreleases/secretary-bernhardt-signs-order-grounding-interiors-drone-fleet-non-emergency

- NPR: "DOI grounds Chinese-made drones" - 1/20
    - https://www.npr.org/2020/01/29/800890201/interior-department-grounds-all-of-its-drones-citing-cybersecurity-other-concern

- USA PATRIOT Act - 10/01
    - https://www.justice.gov/archive/ll/highlights.htm